DRN-5015745

The complaint

Mr S complains that Revolut Ltd won't reimburse him after he fell victim to an investment scam.

Mr S is professionally represented in bringing his complaint to our service, but for ease of reading I'll refer to all submissions as being made by Mr S directly.

What happened

Mr S has explained that in around March 2023, a friend advised him of an investment opportunity he had come across. Mr S researched their website and found it to be professional in appearance. He therefore left his details on an enquiry form and was later contacted by an individual purporting to be a 'broker' for the company. Unfortunately, unbeknownst to Mr S at the time, the 'broker' was in fact a fraudster and the firm he pretended to work for was part of the scam.

Mr S was told he needed to make an initial payment of £100 (which he paid via another bank account provider) and provide documentation for verification. After this Mr S began making further deposits to fund his 'investment' by card payment to a cryptocurrency platform from his Revolut account. The payments Mr S made towards the scam are as follows:

Date	Payment value	Additional comments
27 March 2023	£0.10	Payment reverted
27 March 2023	£4,998	Payment reverted
27 March 2023	£4,998	
14 April 2023	£3,089.70	
16 April 2023	£35.27	
16 April 2023	£2,059.80	

Mr S was led to believe his broker was trading daily for him and that his profits were accumulating. However, when Mr S attempted to make a withdrawal from his account, the fraudster told him there were various fees he would need to first pay. Mr S realised at this point he had fallen victim to a scam. Mr S contacted Revolut on the app-chat to raise a scam. He was told to raise a chargeback for the disputed payments, and did this for one of them. He contacted Revolut again and Revolut asked for more information, including screenshots of the calls he'd had with the fraudster. However, Mr S said he hadn't spoke to the fraudster for weeks and was unable to provide these and as a result, his scam claim wasn't taken further.

Mr S then raised a complaint against Revolut. Revolut didn't uphold Mr S' complaint. It said the chargeback process was cancelled as Mr S only provided limited information. Mr S remained unhappy and referred his complaint to our service. An investigator looked into Mr S' complaint and upheld it in part. She said that Revolut didn't do enough to ensure that Mr S wasn't at risk from financial harm from fraud, as the payments were out of character for his account and were identifiably being made to a cryptocurrency provider – known for carrying a higher risk of fraud. However, she also considered Mr S didn't do enough to protect himself

– by failing to carry out sufficient independent research on the website he was using, prior to making payments. She therefore thought both parties should be equally liable, with Revolut refunding 50% of Mr S' losses.

Mr S agreed with the investigator's view but Revolut didn't. In summary it said:

- Revolut recognises its obligations to have adequate procedures in place to counter the risk that it may be used to further financial crime, but that duty does not go as far as to require Revolut to provide Mr S with a tailored warning. It must comply with valid payment instructions and does not need to concern itself with the wisdom of those instructions. This was confirmed in the recent Supreme Court judgement in the case of *Philipp v Barclays Bank UK plc [2023] UKSC 25*.
- Our service has overstated Revolut's duty to Mr S, and erred in law, by stating that Revolut ought to have done more in this case.
- Revolut has adequate systems and controls in place to detect unusual or suspicious transactions, but these payments were consistent with prior customer instructions and the company was not known to be a scam.
- As payments were made by card, Revolut does not have the option of pausing these while enquiries are made – it can only accept or deny the card payments.
- These were self-to-self payments, and therefore any liability for losses should be split equally between all financial institutions involved.

As no agreement could be reached, the case was passed to me for a decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in *Philipp v Barclays Bank UK PLC*, subject to some limited exceptions, banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In *Philipp*, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to

decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Mr S modified the starting position described in *Philipp,* by – among other things - expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*" (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in March 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[1]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

[1] For example, Revolut's website explains it launched an automated anti-fraud system in August 2018:
https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks_/

For example, it is my understanding that in March 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3).
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms".*
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.
- The October 2017, BSI Code[2], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[3] when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.
- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain

[2] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

[3] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in March 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in March 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Mr S was at risk of financial harm from fraud?

It isn't in dispute that Mr S has fallen victim to a cruel scam here, nor that he authorised the payments he made by card to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in this decision the circumstances which led Mr S to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr S might be the victim of a scam.

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that payments would be credited to a cryptocurrency wallet held in Mr S' name.

By March 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings

about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions[4].

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr S made in March 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in March 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained, Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks. So I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr S might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that all payments were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider), which was a new form of spending for Mr S' account. Additionally, the first successful payment Mr S makes is significantly higher than any other payment that had debited his account in the previous six months (the next highest being a payment transfer of £320). He also had only made one other card payment in the past six months, which was for under £5.

Given what Revolut knew about the destination of this first payment, I think that the overall circumstances should have led Revolut to consider that Mr S was at heightened risk of

---

[4] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Mr S before this payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

What did Revolut do to warn Mr S and should it have done more in the circumstances?

Revolut did not provide warnings for any of the payments Mr S made towards the scam, so I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's primary duty to make payments promptly.

Taking that into account, I think Revolut ought, when Mr S attempted to make the 27 March 2023 payment, knowing that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software, and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mr S by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a cryptocurrency investment scam warning, would that have prevented the losses Mr S incurred?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr S' payments, such as the use of an account manager and the initial low deposit quickly increasing in value.

Mr S has explained that he mostly spoke to the fraudsters by phone and therefore there is less available evidence of how he and the fraudster interacted. However, I've considered that the fraudster's 'spell' was broken when Mr S was told he had to pay a fee before he could withdraw his funds. I think that as Mr S was able to identify this request as

unreasonable and not persist further with payments in a bid to recoup funds already sent, this suggests that he wasn't so taken in by the guidance of the fraudster that he was closed to other possibilities. I think this also refutes Revolut's consideration that Mr S would've ignored guidance it provided on the basis that he had signed up to the investment on the recommendation of a friend. While it may have provided him initial confidence to sign up to the investment, the friend's recommendation doesn't appear to have been so strong that it overrode suspicious requests by the fraudster.

Therefore, on the balance of probabilities, had Revolut provided Mr S with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. He could have paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams. I'm satisfied that a timely warning to Mr S from Revolut would very likely have caused him to take the steps he did take later – revealing the scam and preventing his further losses.

Is it fair and reasonable for Revolut to be held responsible for Mr S' loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr S purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So the funds passed through an additional financial institution before losses were incurred.

I have carefully considered Revolut's view that in a multi-stage fraud, liability for any losses incurred should be split between all financial institutions involved.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr S might have been at risk of financial harm from fraud when he made the first payment towards the scam, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Mr S suffered. The fact that the money wasn't lost at the point it was transferred to Mr S' own cryptocurrency account does not alter that fact and I think Revolut can fairly be held responsible for Mr S' loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr S has only complained against Revolut about the money he lost from this account. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr S could instead, or in addition, have sought to complain against those firms. But Mr S has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr S' compensation in circumstances where Mr S has chosen to only complain about Revolut and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr S' loss from the first successful payment he made to the scam (subject to a deduction for Mr S' own contribution which I will consider below).

Should Mr S bear any responsibility for his losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I recognise that there were aspects to this scam that would have appeared convincing. Mr S has provided evidence that the fraudster provided him with a website, which, while no longer active, Mr S has said appeared legitimate in appearance. He has also explained he was shown graphs depicting the change in cryptocurrency values. Mr S was also introduced to this scam by a friend and while that friend had not withdrawn returns at this point, I can understand why Mr S would be reassured by someone he knows also considering the opportunity to be legitimate.

So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mr S to be reduced. I think it should.

While I accept Mr S had received a recommendation from a friend, Mr S doesn't appear to have conducted any independent research into the firm he believed he was investing in, other than reviewing the website provided to him. Had he reviewed the firm on an online search engine, I can see that by the time Mr S had began making payments there were already a number of negative online reviews, confirming this to be a scam.

Additionally, while we don't have evidence of the majority of the conversations held between Mr S and the fraudster, I have seen one message where Mr S has said '*Just seen my account WOW'.* I think this indicates that Mr S was likely shown impressive returns on his investment (which would also tie in with why he would be wishing to withdraw funds), despite having only begun investing for less than a month. While I accept cryptocurrency exchanges can be volatile, I think a level of returns worthy of withdrawing within weeks ought to have caused Mr S to pause and question the likelihood of the investment being genuine.

I've concluded, on balance, that Revolut can fairly reduce the amount it pays to Mr S because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Could Revolut have done anything else to recover Mr S' money?

I've also thought about whether Revolut could have done more to recover the funds after Mr S reported the fraud.

Payments were made by card to a cryptocurrency provider and that cryptocurrency was sent on to the fraudsters. So, Revolut would not have been able to recover the funds.

In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that the cryptocurrency platform performed its given role in providing cryptocurrency in return for payment in sterling.

Overall I think a fair outcome in this complaint is for Mr S and Revolut to be equally liable for all losses Mr S incurred from his Revolut account and for Revolut to reimburse him 50% of these losses.

My final decision

My final decision is that I uphold Mr S' complaint in part. I require Revolut Ltd to reimburse Mr S:

- 50% of losses incurred to the scam (totalling £5,091.38)

- Apply 8% simple interest per year on that amount from the date of each payment to the date of settlement

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 6 November 2024.

Kirsty Upton
Ombudsman